Louis Daniel Smith, *Pro Se*
C/o: 1314 S. Grand Blvd. Ste 2-128
Spokane, Washington 99202
(509) 590-2188

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WASHINGTON
(Hon. Rosanna Malouf Peterson)

UNITED STATES OF AMERICA Plaintiff, v. LOUIS DANIEL SMITH - 1, Defendant.	**NO: CR-13-00014-RMP** **MOTION TO DISMISS FOR BREACH OF ATTORNEY CLIENT PRIVILEGE OR, IN THE ALTERNATE, TO SUPPRESS THE FRUITS OF THE GOOGLE WARRANT AS TAINTED EVIDENCE** June 9, 2014, 6:30 p.m. Without oral argument.

COMES NOW, Louis Daniel Smith, hereinafter the undersigned, to file the above-captioned motion. In support hereof, the undersigned *declares*, pursuant to 28 U.S.C. § 1746, the following:

On June 28, 2011, Magistrate Cynthia Imbrogno approved a search warrant application submitted by Special Agent Dali Borden (FDA) requesting authorization to search and seize electronically stored information from premises controlled by Google, Inc. A true and correct copy of the Warrant is attached hereto as **Exhibit A** and included herein by reference.

On June 30, 2011 the search warrant was faxed to Google Inc. The warrant was returned roughly five months later on or about November 28, 2011. ECF No. 230-3 at 2 and ECF No. 230-4

According to Agent Borden's January 30, 2012 "Report of Investigation", FDA Document #201202: "The Google search warrant response was directed to [Special Agent] Blenkinsop, an FDA Office of Criminal Investigations computer forensic agent, for preliminary review." A true and correct copy of the relevant portions of Agent Borden's report, as provided by the government in discovery, is attached hereto as **Exhibit B** and included herein by reference.

Senior Special Agent Robert Blenkinsop

Agent Blenkinsop maintains a profile at "Linked-In" (linkedin.com), an online professional networking website, where he lists his work history between 1993-1999 as a Deputy U.S. Marshal and from 1999 to present (14+ years) as a "Senior Special Agent" for the FDA Office of Criminal Investigations in San Francisco. A true and correct copy of Agent Blenkinsop's public profile as printed from the web (last visited 5/9/2014) is attached hereto as **Exhibit C** and included herein by reference.

Agent Borden's Google search warrant affidavit shows that FDA Senior Special Agent Blenkinsop assisted in the government's investigation leading up to his review of the Google return. ECF No. 230-1 at Pp. 33-34. Agent Blenkinsop is mentioned no less than eight (8) times in Agent Borden's affidavit and appears in the search warrant affidavits for 2019 West Riverside (Case No. MJ-11-273-00), 715 West Second (Case No. MJ-11-274-00), 3715 East Longfellow (Case No. MJ-11-282-00), and roughly seventy-eight warrants to search various parcels (Case Nos. MJ-11-294-00 thru MJ-11-371-00).

According to Agent Borden's August 11, 2011 "Report of Investigation", FDA Document #196448, Senior Special Agent Blenkinsop took take part in the FDA's raid of Mr. Smith's home on June 29, 2011. A true and correct copy of the relevant portions of Agent Borden's report, as provided by the government in discovery, is attached hereto as **Exhibit D** and included herein by reference.

According to a "Detail Inventory Listing of All Items at Search Warrant Site", Senior Special Agent Blenkinsop also took part in the FDA's raid of 3715 E. Longfellow. *See* Case No. MJ-11-272-00. A true and correct copy of the Detail Inventory Listing, as provided by the government in discovery, is attached hereto as **Exhibit E** and included herein by reference.

Senior Special Agent Robert Blenkinsop is more than a mere "computer forensics agent" as exhibited by the fact that he initiates investigations (*See* **Exhibit F** at Para. 14.), conducts controlled purchases (*Id.* Para. 15.), reviews website marketing materials for violations (*Id.* Para. 16.), examines product labels (*Id.* Para. 17.), submits chemical samples for laboratory analysis (*Id.* Para. 18.), reviews import records (*Id.* Para. 30.), conducts on-site surveillance (*Id.* Para. 32.), and regularly takes part in FDA raids (as he did on at least two occasions in the instant case, *supra*). It appears that Senior Special Agent Robert Blenkinsop just happens to *also* know a thing or two about computers.

Special Agent Lisa Hartsell

The Court may notice that the aforementioned **Exhibit F** is a search warrant application for an entirely unrelated case, but exhibits that Senior Special Agent Blenkinsop has a close working relationship with Special Agent Lisa Hartsell, the agent applying for the search warrant in **Exhibit F**. According to Agent Borden's August 11, 2011 "Report of Investigation" (**Exhibit D**), Lisa Hartsell *also* took part

in the FDA's raid of Mr. Smith's home on June 29, 2011. According to Agent Borden's affidavit (ECF No. 230-1 at Para 43-44), Ms. Hartsell also took part in the ongoing investigation, and appears in the search warrant affidavits for 2019 West Riverside (Case No. MJ-11-273-00), 715 West Second (Case No. MJ-11-274-00), 3715 East Longfellow (Case No. MJ-11-282-00), and roughly seventy-eight warrants to search various parcels (Case Nos. MJ-11-294-00 thru MJ-11-371-00).

According to Agent Borden's November 29, 2010 "Report of Investigation", FDA Document #181135, Ms. Hartsell also became a private member of Project GreenLife's Private Healthcare Membership Association in order to acquire MMS from PGL in November of 2010. A true and correct copy of the relevant portions of Agent Borden's report, as provided by the government in discovery, is attached hereto as **Exhibit G** and included herein by reference.

It is clear that Senior Special Agent Robert Blenkinsop, Agent Lisa Hartsell, and Agent Dali Borden all worked very closely together during their investigation that led to the instant case. As stated prior, according to Agent Borden's January 30, 2012 "Report of Investigation" **(Exhibit B),** the Google search warrant response was directed to Senior Special Agent Robert Blenkinsop, and yet where attorney-client privileged material known to exist within the return was not filtered prior.

Agent Borden and the government was aware that Project GreenLife consulted with Attorney Nancy Lord, M.D., during the course of the FDA's investigation. *See e.g.,* ECF No. 230-1 at Para 29 ("On August 11, 2010, while the inspection was still underway, the FDA Public Affairs office received a telephone call from attorney Nancy Lord, advising she represented PGL."). Much of PGL's, and thus Mr. Smith's interactions with Attorney Nancy Lord took place via email. These emails invariably contained privileged information regarding Mr. Smith's strategy or position as it

relates to the instant case. The importance of this privilege was recognized by the District Court when it appointment independent third party, Lee Edmond, *Esq.*, to review potentially privileged materials. ECF No. 215. Nevertheless, in *Briggs v. Goodwin*, 698 F.2d 486, 494-95 (1983), the Court said:

> "[O]nce the investigatory arm of the government [*e.g.*, the FDA] has obtained [privileged] information, that information may reasonably be assumed to have been passed on to other governmental organs responsible for prosecution. Such a presumption merely reflects the normal high level of formal and informal cooperation, which exists between the two arms of the executive." *Id.*

Senior Special Agent Robert Blenkinsop was not an independent third party conducting an independent review, but a fully engaged FDA law enforcement officer with a fully vested interest in the case **and unfettered access to Mr. Smith's privileged correspondence.**

Given that Sections I(D-F) and III(A-B) of the Warrant (**Exhibit A**) provided very specific instructions for the reviewing party, and that Section I(E) of the Warrant required that the affidavit be attached to the Warrant, it must be presumed that Agent Blenkinsop read the affidavit and *knew* there would likely be items contained in the return that were protected by attorney-client privilege, thus disqualifying him from reviewing the *unfiltered* data. The government could have *easily* directed the Google return to someone other than a fully vested investigator to first filter out attorney-client emails (like the government contractor who later *did* process the emails) or anyone who was not so obviously invested in the case, **but this is not what happened.**

It can and must be reasonably presumed that Senior Special Agent Robert Blenkinsop's unfettered access to Mr. Smith's privileged correspondence resulted in a breach of attorney-client privilege by the investigatory arm of the government, and

that any number of privileged tidbits of information bearing on defensive "strategy or position" were either passed on to Blenkinsop's teammates, Agents Borden and Hartsell, or that between any three of them, such information, whether intentional or not, whether subtly or overtly, was passed on to individuals responsible for prosecution. The *Briggs* Court noted, "such a presumption merely reflects the normal high level of formal and informal cooperation, which exists between the two arms of the executive." *Id.* 698 F.2d 486 at 494-95. The *Briggs* Court also stated:

> "The prosecution makes a host of discretionary and judgmental decisions in preparing its case. It would be virtually impossible for an appellant or a court to sort out how any particular piece of information in the possession of the prosecution was consciously or subconsciously factored into each of those decisions. Mere possession by the prosecution of otherwise confidential [495] knowledge about the defense's **strategy or position** is sufficient in itself to establish detriment to the criminal defendant. Such information is 'inherently detrimental, . . . unfairly advantages the prosecution, and threatens to subvert the adversary system of criminal justice.'" (*Quoting State v. Lenarz*, 301 Conn. 417) *Id.* 698 F.2d 486 at 494-95 [Emphasis supplied.]

In *State v. Lenarz*, 301 Conn. 417 (2011), the Court held that "the taint caused by the state's intrusion into the [attorney-client] privileged communications would be **irremediable** on retrial and the charge of which the defendant was convicted must be dismissed." [Emphasis supplied.]

Government Trial Attorney Kathryn Drenning

In a latent show of alleged "protection" of Mr. Smith's attorney-client privilege, a privilege that had already been breached by the FDA, the prosecution team appointed Kathryn Drenning, a trial attorney who conveniently works in the same office and along-side the prosecution, to conduct a red herring "privileged review" while USPS and FDA field agents retained complete unfiltered copies of all privileged material.

Ms. Drenning tagged roughly 1260 emails as "potentially privileged" that Special Master, Lee Edmond, *Esq.*, would later review. ECF No. 295.

Government Trial Attorney Jeffrey Steger

Trial Attorney Jeffrey Steger, who works directly with Christopher E. Parisi's (the government's prosecutor in this case) works closely with Kathryn Drenning. Trial Attorneys Drenning and Steger are presently prosecuting two cases in the Southern District of Florida (Case Nos. 0:2012-cr-60186 and 1:2013-cr-20834), where Mr. Parisi is trying a similar case (Case No. 0:2013-cr-60156).

Moreover, Jeffrey Steger was FDA Agent Borden's *primary* contact at D.O.J. prior to Mr. Parisi being assigned to the case. *See* **Exhibit H**, a true and correct copy of Agent Borden's ROI_030211 (Pp. 3-4), as provided by the government in discovery:

> "On 01/21/11, **SA Borden was contacted by OCL Attorney Jeff Steger inquiring about the investigation.** Steger indicated he would consult with his supervisor and likely contact AUSA Harrington, EDWA, **to see if Steger could be of assistance.**"
>
> "On 02/01/11, **Jeff Steger, OCL, contacted SA Borden** after he consulted with AUSA Harrington, EDWA. **Steger had contacted the AUSA to offer assistance** in the EDWA investigation if Harrington was ready to pursue the case or **to advise Harrington of OCL's interest in the investigation. Steger advised SA Borden** that AUSA Harrington wanted to have a conference call to review the status of the investigation on 02/08/11."
>
> "From 02/02 to 02/04/11, SA Borden assembled a briefing document regarding the investigation to date, for the conference call."
>
> "On 02/08/11, **SA Borden organized a conference call with the AUSA from EDWA, Trial Attorney Steger, OCL, Jim Smith, OCC, and Investigator Bega, USPIS. The attorneys and investigators discussed the investigation** to date and **the attorneys asked questions related the violations of the FDCA.**"

> "02/15/11, **Trial Attorney Steger, OCL, advised SA Borden that OCL would take the lead on this investigation. Trial Attorney Chris Parisi had been assigned the case and will be working on the matter.** EDWA has offered administrative support and help with Grand Jury, subpoenas, and anything else that comes up."

It is clear from all the above, Attorneys Jeffrey Steger and Christopher Parisi are both connected to and have an interest in the outcome of this case. It is also clear that the government's "privilege review" attorney, Kathryn Drenning, works closely with and has an interest in the litigation activities of Jeffrey Steger, who instigated the department's involvement in this case and who works directly with Christopher Parisi, who is trying a similar case as Mr. Steger and Ms. Drenning are together trying in the Southern District of Florida. In other words, Kathryn Drenning, *who has personally reviewed all attorney-client privileged emails in this case*, is not even remotely removed from the instant case being a trial attorney working hand in hand with the prosecution team and whose office has a financial stake in the outcome of this case. One would not be mistaken to liken it unto a fox guarding the hen house. Again, as the Court stated in *Briggs*:

> "Once the investigatory arm of the government has obtained information, that information may reasonably be assumed to have been passed on to other governmental organs responsible for prosecution. Such a presumption merely reflects the normal high level of formal and informal cooperation which exists between the two arms of the executive." *Id.* 698 F.2d 486 at 494-95.

While *Briggs* assumes a breach of privilege under the FDA's and Senior Special Agent Robert Blenkinsop's unfiltered review, how much more may we 'reasonably assume' that privileged information has been passed onto the prosecution if it is also in the possession of and has been reviewed by Mr. Steger's and Mr. Parisi's associate, Ms. Drenning, whom together, are all trial attorneys working together in the same office and have similar interests in the outcome of this and other

cases they are trying together? How could Ms. Drenning be considered anything close to an impartial third party, such as the Court appointed Discovery Master, Lee Edmond, *Esq.*? The answer is, she can't! Like Senior Special Agent Robert Blenkinsop before her, Ms. Drenning possesses an inherent and insurmountable conflict of interest.

Despite this fact, the government's *ex post facto* "privileged review" by Ms. Drenning is nothing more than a red herring that takes the focus off the FDA's prior unfettered review by Senior Special Agent Robert Blenkinsop.

Again, "Moreover, the [defendant] need not prove that the prosecution actually used the information obtained. The prosecution makes a host of discretionary and judgmental decisions in preparing its case. It would be virtually impossible for an appellant or a court to sort out how any particular piece of information in the possession of the prosecution was consciously or subconsciously factored into each of those decisions. Mere possession by the prosecution of otherwise confidential knowledge about the defense's **strategy or position** is sufficient in itself to establish detriment to the criminal defendant. Such information is 'inherently detrimental, . . . unfairly advantages the prosecution, and threatens to subvert the adversary system of criminal justice.'" *Briggs*, 698 F.2d 486 at 494-95 [Emphasis supplied.]

In *United States v. Danielson*, 325 F.3d 1054 (9th Cir. 2003), the Court said:

> "The government's interference with Danielson's attorney-client relationship was neither accidental nor unavoidable, but was rather the result of deliberate and affirmative acts. We therefore hold that if there was prejudice there was a violation of the Sixth Amendment under *Weatherford v. Bursey*, 429 U.S. 545, 51 L. Ed. 2d 30, 97 S. Ct. 837 (1977). For a determination of prejudice, we rely on *United States v. Mastroianni*, 749 F.2d 900 (1st Cir. 1984), and *Kastigar v. United States*, 406 U.S. 441, 32 L. Ed. 2d 212, 92 S. Ct. 1653 (1972), to hold that the government has the '**heavy burden**' of proving non-use of Danielson's trial strategy information." [Emphasis supplied.]

The burden is heavy for the government to illustrate *pretrial* no potential prejudice to Mr. Smith for its breach of attorney-client privilege by both the investigatory arm and the very department responsible for prosecution.

The government has been privy to and exposed to not only "strategy" but also "position" (as worded in *Briggs* and *Lenarz*), creating a presumption *pretrial* of a major violation of Mr. Smith's attorney-client privilege and due process rights. The department's "tasking" of Trial Attorney Kathryn Drenning to conduct a "privilege review" after the FDA already enjoyed unfettered access to privilege material, cannot begin to substitute for the right of due process owed to Mr. Smith.

The undersigned, not being a lawyer, admittedly does not know where to look in the Ninth Circuit for a case wholly apposite to the circumstances of the instant case. The undersigned, however, believes that the executive branch owed Mr. Smith a far greater duty under the Sixth Amendment and the rules of substantive and procedural due process, than to give both the FDA, and the same office prosecuting him, unfettered access to electronic information known entirely before-hand to contain attorney-client privileged information.

In the very least, the Google return should have been directed to a Court appointed independent third party, such as Lee Edmond, *Esq.*, or the government's contractor, to filter emails between Mr. Smith and Attorney Nancy Lord, M.D., **from the very beginning** rather than in the end.

That is the very kind of thing the guidance offered by the Ninth Circuit in *Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010) could have helped avoid. In *CDT*, the Court said that an issuing judicial officer of a warrant seeking electronic information should insert, "a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable

cause is shown" and "where privacy interest of numerous other parties who are not under suspicion of criminal wrongdoing [*i.e.,* Project GreenLife Association Members] are implicated by the search, the presumption should be that segregation of the data will be conducted by an independent third party selected by the court." *Id.,* at 1179. The Ninth Circuit also said, "the government agents involved in the investigation should be allowed to examine *only* the information covered by the terms of the warrant" and "[t]he government should not retain copies of such [unauthorized] data unless it obtains specific judicial authorization to do so." *Id.,* at 1179. The Court also said, "the return should include a sworn certificate that the government has destroyed or returned all copies of data that it is not entitled to keep." *Id.,* at 1179.

Chief Judge Kozinski said that this guidance "offer[ed] the government a safe harbor, while protecting the people's right to privacy and property in their papers and effects". *Id.* at 1178. Had the Ninth Circuit's guidance been followed from the beginning, it would not have only protected Mr. Smith's privacy as it relates to *non-privileged* material, but also where it relates to those items and information know by the government from the outset to be protected under the attorney-client privilege.

WHEREFORE the undersigned respectfully requests the Honorable Court to dismiss this case for breach of attorney-client privilege, or in the alternate, to suppress the Google return as tainted evidence similar to that as was done in *United States v. Renzi,* 722 F. Supp. 2d 1100 (9th Cir. 2010) wherein, after *de novo* review, the court adopted the magistrate's report and recommendation as the opinion of the court, denying the motion to dismiss based on the government's unlawful recording of privileged counsel calls as part of a wiretap but granting as to suppression of *all* evidence obtained by the wiretap.

Dated and executed this 9 Day of May 2014 *A.D.*

Respectfully submitted,

By: _____

Louis Daniel Smith, *Pro Se*
C/o: 1314 S. Grand Blvd. Ste 2-128
Spokane, Washington 99202
(509) 590-2188

VERIFICATION AND DECLARATION

IT IS HEREBY certified and declared pursuant to 28 U.S.C. § 1746 (without the United States) that the contents of the foregoing motion are true and correct under the penalties of perjury to the best of my knowledge and belief and that the exhibits hereto are true and correct copies (redacted where apprpriate) as printed from their respective sources.

Dated and executed this 9 Day of May 2014 *A.D.*

By: _____

Louis Daniel Smith
C/o: 1314 S. Grand Blvd. Ste 2-128
Spokane, Washington 99202
(509) 590-2188

CERTIFICATE OF SERVICE

IT IS HEREBY certified that on the 7 Day of May, 2014 *A.D.*, the foregoing motion was deposited with the Clerk of the Court for filing with the CM/ECF system, which will send notification of such filing to the following parties whom are all CM/ECF participants.

Christopher E. Parisi
U.S. Department of Justice
Liberty Square Bldg, Rm. 6400
450 Fifth Street NW
Washington, D.C. 20530
(202) 598-2208
christopher.e.parisi@usdoj.gov

Timothy T. Finley
U.S. Department of Justice
DC Consumer Protection Branch
P.O. Box 386
Washington, DC 20044-0386
(202) 307-0050
timothy.t.finley@usdoj.gov

Virginia Rockwood
Attorney at Law
P.O. Box 10258
Spokane, WA 99209
(509) 993-1601
virginiarockwood@gmail.com

Bevan Jerome Maxey
Maxey Law Offices
1835 W Broadway
Spokane, WA 99201
(509) 326-0338
hollye@maxeylaw.com

Nicolas V. Vieth
505 W Riverside, Ste 200
Spokane, WA 99201
(208) 664-9494
nick@viethlaw.com

Terence Michael Ryan
1304 W College Avenue
Spokane, WA 99201-2013
(509) 325-5466
tryan@qwestoffice.net

By: _____

Louis Daniel Smith, *Pro Se*
C/o: 1314 S. Grand Blvd. Ste 2-128
Spokane, Washington 99202

(509) 590-2188

EXHIBIT A

A - COPY

AO 93 (12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Washington

In the Matter of the Search of
Information Associated with User Accounts that are stored at the Premises Controlled by Google.

Case No. 11J-11-272-0

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the EASTERN District of WASHINGTON (*identify the person or describe the property to be searched and give its location*): See Attachment A, which is herein incorporated by reference,

The person or property to be searched, described above, is believed to conceal (*identify the person or describe the property to be seized*): See Attachment A, which is herein incorporated by reference, which items are evidence of violation(s) of 21 USC 331(a), 331(d), 18 USC 545 + may be seized.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before July 11, 2011
(*not to exceed 14 days*)

☒ in the daytime 6:00 a.m. to 10:00 p.m.

☐ at any time in the day or night as I find reasonable cause has been established

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Cynthia Imbrogno.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*)
☐ for _____ days (*not to exceed 30*).
☐ until, the facts justifying, the later specific date of _____.

Date and time issued: June 28, 2011 at 10:39 a.m.

Judge's signature

City and state: Spokane, Washington

Cynthia Imbrogno, United States Magistrate Judge
Printed name and title

The search shall be conducted in a manner to reasonably protect the privacy interests of innocent 3rd parties & in a manner so as not to disrupt lawful business unreasonably. CLOSED Transaction.

AO 93 (Rev. 01/09) Search and Seizure Warrant (Page 2)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

For the time period covering August 11, 2007, to the date this warrant is received:

Section I. Search Procedure

A. The search warrant will be presented to Google personnel who will be directed to isolate those account(s) and file(s) described in Section II below;

B. In order to minimize any disruption of computer service to innocent third parties, Google employees and law enforcement personnel trained in the operation of computers will collect information, including emails and talk content, only related to the account(s) and files described in Section II below;

C. Google employees will provide the exact duplicate in electronic form of the account(s) and electronic file(s) described in Section II below and all information stored in those account(s) and file(s) to the agent who serves this search warrant;

D. Law enforcement personnel will thereafter review the information stored in the account(s) and file(s) received from Google employees and identify and copy the information contained in those accounts and files which are authorized to be further copied as described in Section III below; and

E. In the event that agents examining the data and/or information provided by Google Inc., discover, in plain view, evidence of criminal conduct other than that described in ~~this~~ the affidavit, the examiner shall not ~~seize such~~ search for or data and/or

attached to the search warrant application contained

information until a supplemental search warrant is obtained which specifically authorizes the seizure of such data and/or information related to other crimes. search for and/or

F. Law enforcement personnel will then seal the original duplicate of the account(s) and file(s) received from Google employees and will not further review the original duplicate absent an order of the Court.

G. A copy of the warrant will be left with Google employees to serve as notice of the execution of the warrant.

Section II. Files and Accounts to be Copied by Google Employees

A. Any and all documents, data, records, and information related to Google Apps for Business accounts for "Project Greenlife," "PGL International LLC," or accounts in the names of "L. Daniel Smith," "Daniel Votino," or "Karis Delong," including but not limited to the account(s) "joe.PGL@gmail.com," "joe@projectgreenlife.com," "Daniel (PGL) [daniel@projectgreenlife.com]," "dvotino@gmail.com," MMS Miracle <mmsmiracle@gmail.com, customercare@projectgreenlife.com, to include all subscriber information such as name, address, date of birth, gender, date of account creation, account status, Google email address(es) alternate email address(es), registration from IP address, date ID registered, IP addresses associated with the session times and data, and any and all methods of payment provided by the subscriber to Google for any

premium services;

B. For the subscriber(s) identified in Section II(A) above, the contents of any and all emails, chats, and other correspondence stored in the subscriber's Google account(s);

C. Any and all contents of electronic fields that the subscriber has stored in the subscriber's Briefcase and Photo area;

D. Any and all Google IDs listed on the subscriber's Friends list;

E. All existing printouts from original storage of all the electronic mail described in Section II(A);

F. All transactional information of all activity of the email address(es) and/or individual connection, ports, dial-ups, and/or locations;

G. All business records and subscriber information, in any form kept, pertaining to the email address(es) and/or individual account(s) described in Section II(A), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records; and;

H. All records indicating the services available to the subscribers of the email address(es) and/or individual account(s) described above in Section II(A).

Section III. Information to be Further Copied and Analyzed by Law Enforcement Personnel

A. Law enforcement personnel will review the information received from Google and identify and copy information regarding any and all fruits, instrumentalities, evidence, documents, data, and records relating to smuggling, misbranding, and new drug violations between the dates of August 11, 2007 through the date of subpoena compliance including:

1. Any and all correspondence and/or files regarding the purchase, manufacture, sale of MMS, movement of funds related to MMS, sodium chlorite that is ordered or imported, or correspondence and/or files responding to inquiries from FDA or the U.S. Customs and Inspection Service regarding imported sodium chlorite, including all opened and unopened email;
2. Any and all correspondence and/or files regarding the issues discussed in paragraph III(A)(1);
3. Internet account information, to the extent available, including dates and times of activity of "joe.PGL@gmail.com, "joe@projectgreenlife.com", "Daniel (PGL) [daniel@projectgreenlife.com]", "dvotino@gmail.com," "MMS

Miracle <mmsmiracle@gmail.com", and "customercare@projectgreenlife.com."

B. Law enforcement personnel will then seal the original duplicate of the account(s) and file(s) received from Google employees and will not further review the original duplicate absent an order of the Court.

C. The Internet Protocol (IP) addresses with their dates and times, if available, used to send, check, or receive email using the accounts "joe.PGL@gmail.com, "joe@projectgreenlife.com", "Daniel (PGL) [daniel@projectgreenlife.com]", "dvotino@gmail.com", "MMS Miracle <mmsmiracle@gmail.com", and customercare.projectgreenlife.com.

D. The IP addresses, if available, used to create or modify the accounts "joe.PGL@gmail.com, "joe@projectgreenlife.com", "Daniel (PGL) [daniel@projectgreenlife.com]", "dvotino@gmail.com", "MMS Miracle <mmsmiracle@gmail.com", and "customercare@projectgreenlife.com."

E. All transactional information of all activity of the email account / address described in item A of this Attachment 1, and any associated account, including log files, dates, times, methods of connecting, ports, and IP addresses.

F. All business records and subscriber information, in any form kept, pertaining to the email account / address described in item A of this Attachment 1, and any

associated account, including account applications, subscriber's names, screen names, all account names associated with the subscriber(s), telephone numbers, addresses, and passwords.

EXHIBIT B

B

Food and Drug Administration
OFFICE OF CRIMINAL INVESTIGATIONS
REPORT OF INVESTIGATION

REPORTING OFFICE:	Seattle Domicile Office
DOCUMENT NUMBER:	20/202
CASE NUMBER:	2011-SEW-715-0059
RELATED CASE NUMBER:	
TYPE OF CASE:	715.100, MISBRANDED PRODUCTS - CDER
CASE TITLE:	PROJECT GREEN LIFE
CASE AGENT:	DALI BORDEN
INVESTIGATION MADE AT:	Kirkland, WA
INVESTIGATION MADE BY:	SA DaLi Borden
REPORTING PERIOD:	**FROM:** 11/11/2011 **TO:** 01/30/2012
STATUS OF CASE:	Continued
SYNOPSIS:	Google search warrant information received. Tamara Olson started online company selling MMS.

RESTRICTED INFORMATION

This report is furnished on an official need-to-know basis and must be protected from dissemination which might compromise the best interests of the Food and Drug Administration, Office of Criminal Investigations. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the FDA Office of Criminal Investigations.

UNAUTHORIZED RELEASE MAY RESULT IN CRIMINAL PROSECUTION

REPORT SUBMITTED BY: _____ DATE: 01/30/2012
DaLi Borden, Special Agent

REPORT APPROVED BY: _____ DATE: 2/2/12
Thomas W. Emerick, Special Agent In Charge

DISTRIBUTION:
ORIG: SFC
CC: LAC
CC: SEW

[redacted]

2. DETAILS OF INVESTIGATION:

On or about November 30, 2011, Google provided a response to a search warrant issued by the U.S. District Court, Eastern District of Washington, on 6/28/11; and served on 6/30/11. The Google search warrant response was directed to SA Blenkinsop, an FDA Office of Criminal Investigations computer forensic agent, for preliminary review. SA Blenkinsop began the initial processing of the evidence provided by Google, pursuant to the search warrant executed on June 30, 2011. SA Blenkinsop located

[redacted]

[redacted]

EXHIBIT C

Robert Blenkinsop

Senior Special Agent at FDA-OCI

San Francisco Bay Area | Law Enforcement

Current	FDA-Office of Criminal Investigations
Previous	United States Marshals Service
Education	University of California, Berkeley

Send Robert InMail

30 connections

Background

Experience

Senior Special Agent
FDA-Office of Criminal Investigations
September 1999 – Present (14 years 9 months) | San Francisco Bay Area

Deputy U.S. Marshal
United States Marshals Service
February 1993 – September 1999 (6 years 8 months) | San Francisco Bay Area

Skills & Endorsements

Top Skills

1 Criminal Investigations
1 Cybercrime
1 Computer Forensics
1 Internet Investigations
1 Computer Security
1 Mobile Devices
1 Active Top Secret...
1 Financial Crime
1 Expert Witness
1 Information Technology

Robert also knows about...

1 Surveillance 1 Fugitive Recovery 1 Firearms Federal Law Enforcement

Education

University of California, Berkeley

Following

Guidance Software
Computer & Network Security
✚ Follow

FDA
Government Administration
✚ Follow

Schools

University of Californ...
San Francisco Bay Area
✚ Follow

EXHIBIT D

D

Food and Drug Administration
OFFICE OF CRIMINAL INVESTIGATIONS
REPORT OF INVESTIGATION

REPORTING OFFICE:	Seattle Domicile Office
DOCUMENT NUMBER:	196448
CASE NUMBER:	2011-SEW-715-0059
RELATED CASE NUMBER:	
TYPE OF CASE:	715.100, MISBRANDED PRODUCTS - CDER
CASE TITLE:	PROJECT GREEN LIFE
CASE AGENT:	DALI BORDEN
INVESTIGATION MADE AT:	Kirkland, WA
INVESTIGATION MADE BY:	SA DaLI Borden
REPORTING PERIOD:	**FROM:** 05/24/2011 **TO:** 08/11/2011
STATUS OF CASE:	Continued
SYNOPSIS:	Search warrants served at SMITH'S and DELONG'S residence, shipping warehouse, and manufacturing facility. Seizure warrants were served for three Wells Fargo bank accounts.

REPORT SUBMITTED BY: _____ DATE: 08/11/2011
DaLI Borden, Special Agent

REPORT APPROVED BY: _____ DATE: 8/11/11
Thomas W. Emerick, Special Agent in Charge

DISTRIBUTION:
ORIG: SFC
CC: LAC
CC: SEW

On 06/29/11, at approximately 8:20 AM, FDA OCI and USPIS executed search warrants at 715 West Second Avenue, Spokane, WA, and 2019 Riverside Avenue, Spokane, WA, for evidence related to violations of 18 U.S.C. 545 Smuggling, and 21 U.S.C . 331(a) and 333. The Affidavit for Search Warrant was sealed by the Magistrate for both locations. See Attachment 1 – Affidavit for Search Warrant for 3715 E Longfellow, Attachment C.

At approximately 9:10 AM "Luna" last name unknown, 360-770-9625, an occupant of the upper level, granted SA's Hartsell and Blenkinsop verbal consent to access the wireless router that was utilized by the whole house. MS. DELONG gave agents consent to search the unattached garage for evidence and no evidence was taken. See Attachment 2 - Consent to Search.

EXHIBIT E

E Borden's

Detail Inventory Listing of All Items at Search Warrant Site

Site Name: 3715 E. Longfellow, Spokane, WA Facility

Investigation Number: 11SEW0059

Starting Date and Time: 06/29/2011 05:05 PM

Ending Date and Time:

Report Date: Wednesday, June 29, 2011

Control #:	1	**Evidence Box:**	1
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Bill of Lading to Chris Olson		
Key Word:	Docs		
Location:	Labeling Room		
Found:	Room AA-2nd Shelf under label applicator		
Locating Investigator:			
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	2	**Evidence Box:**	2
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Box of 19 bottles of PGL MMS		
Key Word:	Product - Wet		
Location:	Upstairs Storage		
Found:	Room GG - On Floor		
Locating Investigator:	Rob Blenkinsop		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	3	**Evidence Box:**	3
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Box containing rolls of labels		
Key Word:	Docs-VSE		
Location:	Boxing Room		
Found:	Room BB - In Box		
Locating Investigator:	Stephen Jackson		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	4	**Evidence Box:**	4
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant 7 boxes of Packaging Material		
Key Word:	Docs-VSE		
Location:	Boxing Room		
Found:	Room BB-On floor		
Locating Investigator:	Lisa Harstell		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	5	**Evidence Box:**	5
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant 2 Trashcans filled with plastic bottles.		
Key Word:			
Location:	Boxing Room		
Found:	Room BB - On Floor		
Locating Investigator:	Stephen Jackson		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	6	**Evidence Box:**	6
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Bottle Caps		
Key Word:			
Location:	Labeling Room		
Found:	Room AA-On floor		
Locating Investigator:	Hilary Rickher		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	7	**Evidence Box:**	7
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant 3 Rolls of Labels		
Key Word:	Docs-VSE		
Location:	Boxing Room		
Found:	Room BB -		
Locating Investigator:	Marc Ruiz		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	8	**Evidence Box:**	8
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Bill of Lading		
Key Word:	Docs		
Location:	Boxing Room		
Found:	Room BB - On Floor		
Locating Investigator:	Jared Friedman		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	9	**Evidence Box:**	9
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Documents		
Key Word:			
Location:	Garage		
Found:	Room EE - On piano		
Locating Investigator:	Jared Friedman		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	10	**Evidence Box:**	10
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Plastic bags and Labels		
Key Word:	Docs-VSE		
Location:	Labeling Room		
Found:	Room AA - Bottom Shelf		
Locating Investigator:	Lisa Harstell		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	11	**Evidence Box:**	11
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Numerical Control liquid filling machine		
Key Word:	Product Equipment		
Location:	Boxing Room		
Found:	Room BB -		
Locating Investigator:	Marcel Korvela		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	12	**Evidence Box:**	12
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Sealed for your protection labels		
Key Word:	Docs-VSE		
Location:	Labeling Room		
Found:	Room AA- Table top		
Locating Investigator:	Lisa Harstell		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	13	**Evidence Box:**	13
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Directions for manufacturing.		
Key Word:	Docs		
Location:	Labeling Room		
Found:	Room AA - in box 2nd shelf		
Locating Investigator:	Lisa Harstell		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	14	**Evidence Box:**	14
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Label Applicator		
Key Word:	Product Equipment		
Location:	Labeling Room		
Found:	Room AA - Countertop		
Locating Investigator:	Lisa Harstell		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	15	**Evidence Box:**	15
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Box of R4 rolls of PGL MMS Labels		
Key Word:	Docs-VSE		
Location:	Upstairs Storage		
Found:	Room GG- On floor		
Locating Investigator:	Rob Blenkinsop		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	16	**Evidence Box:**	16
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Parcel from container 7947 6619 3278		
Key Word:	Docs-VSE		
Location:	Labeling Room		
Found:	Room AA		
Locating Investigator:	France Bega		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	17	**Evidence Box:**	17
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Numerical Control Liquid Filling Machine		
Key Word:	Product Equipment		
Location:	Labeling Room		
Found:	Room AA - Table Top		
Locating Investigator:	Lisa Harstell		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	18	**Evidence Box:**	18
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Box containing caps		
Key Word:	Product Equipment		
Location:	Boxing Room		
Found:	Room BB		
Locating Investigator:	Jared Friedman		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	19	**Evidence Box:**	19
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Shipping Stickers		
Key Word:	Docs-VSE		
Location:	Labeling Room		
Found:	Room BB		
Locating Investigator:	Michael Baxter		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	20	**Evidence Box:**	20
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant	Small Uline Box marked reclosable bags.Ok to ship stickers w/ 3 bottles of Citric Acid	
Key Word:	Product-Dry		
Location:	Labeling Room		
Found:	Room AA		
Locating Investigator:	DaLi Borden		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	21	**Evidence Box:**	21
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant	Bags of Citric Acid	
Key Word:	Product-Dry		
Location:	Wharehouse		
Found:	Room DD		
Locating Investigator:	Marc Ruiz		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	22	**Evidence Box:**	22
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant	Grey Plastic barrel containing unknown liquid.	
Key Word:	Product-Dry		
Location:	Labeling Room		
Found:	Room AA		
Locating Investigator:	Lisa Harstell		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	23	**Evidence Box:**	23
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant	Type Magnetic Induction Sealer	
Key Word:	Product Equipment		
Location:	Labeling Room		
Found:	Room AA - Table Top		
Locating Investigator:	Lisa Harstell		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	24	**Evidence Box:**	24
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Table top Conveyor Belt		
Key Word:	Product Equipment		
Location:	Labeling Room		
Found:	Room AA - Table Top		
Locating Investigator:	Lisa Hairstell		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	25	**Evidence Box:**	25
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant White buckets containing unknown liquid		
Key Word:	Product - Wet		
Location:	Boxing Room		
Found:	Room BB		
Locating Investigator:	Jared Friedman		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	26	**Evidence Box:**	26
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Caged White Vat (Empty) Labeled Sodium Chlorite		
Key Word:	Product Equipment		
Location:	Garage		
Found:	Room EE		
Locating Investigator:	Stephen Jackson		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

Control #:	27	**Evidence Box:**	27
Photo #:		**Locator Code:**	
Description:	Seized Per Warrant Caged White Vat with liquid Labeled Sodium Chlorite		
Key Word:	Product - Wet		
Location:	Wharehouse		
Found:	Room DD		
Locating Investigator:	Stephen Jackson		
Evidence Custodian:	Monique Macaraeg		
Evidence Logger:	Monique Macaraeg		

EXHIBIT F

THIS CASE IS NOT RELATED

JDR

AO 106 (Rev. 01/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of California

FILED

2009 SEP 25 AM 10:04

CLERK US DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY DEPUTY

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
1305 Hot Spring Way, Suite 103
Vista, California 92081

Case No. '09 MJ2843

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Southern District of California *(identify the person or describe property to be searched and give its location):* See Attachment A.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized):* See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 21 U.S.C. § 331 and 841, and the application is based on these facts: See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Lisa Hartsell
Printed name and title

Sworn to before me and signed in my presence.

Date: 9/24/09

Judge's signature

City and state: San Diego, California

United States Magistrate Louisa S. Porter
Printed name and title

ATTACHMENT A

LOCATION TO BE SEARCHED

The premises is located within the Sycamore Pointe Business Park at 1305 Hot Spring Way, Suite 103, Vista, CA. Suite 103 is located on the southwest corner of Hot Spring Way and Sycamore Avenue in Vista, CA. Suite 103 is further described as consisting of 4,639 square feet of warehouse space with a 1,157 square foot office space. The facade of the building is constructed of off white concrete and stacked stone.

Entrance to Suite 103 is through a single glass door. Above the door in white stencil print is "103." A handicap sticker (blue) is located to the right of the door at the height of the door handle/lock. On the plate glass window adjacent to the door is stenciled "Charter Companies Sycamore Pointe Management Office."

ATTACHMENT B

ITEMS TO BE SEIZED

Authorization is sought to search for and seize evidence that I FORCE NUTRITION and TRIBRAVUS ENTERPRISES LLC are involved in the unlawful distribution of misbranded, adulterated, and unapproved drugs, in violation of 21 U.S.C. § 331, as well as the illegal distribution of "Androstenedione,"a controlled substance, in violation of 21 U.S.C. § 841. Authorization to search includes any detached structures from the primary premises if such additional structures exist.

This authorization includes the search of physical documents and includes electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and computer media will be conducted in accordance with the "Procedures For Electronically Stored Information" provided in the affidavit submitted in support of this warrant. Items to be seized include the following:

a. All computer systems, software, peripherals and data storage devices.

b. All documents which evidence violations of 21 U.S.C. § 331 and 21 U.S.C. § 841. which took place from October 1, 2007 to present, including all temporary and permanent electronic files and records relating to:

1. The following unapproved drugs, fraudulently labeled as "dietary supplements", and their packaging, labeling, and containers: I FORCE Dymethazine; I FORCE 1,4 AD Bold 200; I FORCE 17a PheraFLEX; and I FORCE Methadrol;

2. Any and all documents relating to the research, formulation, purchase, distribution, receipt, manufacturing, marketing, and administration of the items listed above at paragraph 1 (or the raw materials used in the manufacture of said items), including records reflecting the monitoring and/or testing of the products themselves;

3. Any and all import records, customs declarations, communications with suppliers of raw materials, related to any of the products listed in paragraph 1 above;

4. Any and all financial records relating to I FORCE, I FORCE NUTRITION, TRIBRAVUS ENTERPRISES, DAVID NELSON and/or any other businesses or entities associated with the above individuals and entities, related to any of the products listed in paragraph 1 above;

5. Any and all records, correspondence, letters, receipts, recordings, messages and information relating to the businesses known as I FORCE, I FORCE NUTRITION, and TRIBRAVUS ENTERPRISES, related to any of the products listed in paragraph 1 above;

6. Address books, phone books, personal calendars, daily planners, journals, itineraries, rolodex indices and contact lists associated with I FORCE, I FORCE NUTRITION, TRIBRAVUS ENTERPRISES, and/or DAVID NELSON;

7. Any records relating to any off-site business locations and/or off-site storage facilities, more particularly described as contracts, receipts, keys, notes, bills and any letters of correspondence, where the above listed items in paragraph 1 may be stored.

c. User-attribution data to include data reflecting who used or controlled the computer or electronic storage device at or around the time that data reflecting criminal activity within the scope of this warrant was created, accessed, deleted, modified, copied, downloaded, uploaded or printed. User-attribution data includes registry information, computer logs, user profiles and passwords, web-browsing history, cookies, electronic mail stored on the computer or device, electronic address books, calendars, instant messaging logs, electronically-stored photographs and video, file structure and user-created documents, including metadata.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Lisa Hartsell, being duly sworn, hereby depose and state:

I. AFFIANT'S BACKGROUND AND REQUEST FOR WARRANT

1. I am a Special Agent for the U.S. Food and Drug Administration ("FDA") Office of Criminal Investigations ("OCI") in San Clemente, California. I have been employed by OCI since October 1997. Prior to my employment with the OCI, I was employed by the U.S. Department of Commerce's Office of Export Enforcement responsible for conducting investigations involving violations of the United States' national security, nonproliferation and foreign policy high technology export controls. I was employed by the U.S. Department of Commerce for thirteen years. I am currently responsible for conducting criminal investigations of violations of Title 18 and 21, United States Code. During my employment with FDA/OCI, I have been involved in criminal investigations involving the distribution of counterfeit and unapproved drugs, dietary supplements, and misbranded and/or adulterated products in violation of 21 U.S.C. § 331, as well as violations of the Federal Anti-Tampering Act, 18 U.S.C. § 1365; violations of the Prescription Drug Marketing Act, 21 U.S.C. § 331(t), and other health care fraud investigations. I am a graduate of the Federal Law Enforcement Training Center and the University of California, and have participated in and directed the conduct of numerous search warrants at a variety of premises including residences and businesses. The majority of these search warrants have involved the seizing of computers and related equipment. I have also consulted with other agents who have conducted similar search warrants. Additionally, through my training as a Special Agent, I have been certified as Seized Computer Evidence Recovery Specialist.

2. This affidavit is made in support of a search warrant for the premises located at 1305 Hot Spring Way, Suite 103, Vista, CA, more fully described in Attachment A. The premises located on Hot Spring Way is the sole location of Tribravus Enterprises, LLC dba I FORCE NUTRITION (I FORCE). This search warrant is sought in connection with an investigation into I FORCE's illegal manufacture and distribution in interstate commerce of misbranded and unapproved new drugs in violation of 21

U.S.C. §§ 331(a), (c), (d), and (k), as well as the illegal distribution of "Androstenedione," a controlled substance, in violation of 21 U.S.C. § 841.

3. Based on my experience and background as a Special Agent for the FDA/OCI, my personal conversations with other FDA/OCI Agents, U.S. Postal Service Postal Inspectors and Drug Enforcement Administration (DEA) Special Agents, and my review of records, I have probable cause to believe that the owner and employees of I FORCE have committed violations of the above-described criminal statutes and that evidence of these violations exist within the location described in Paragraph 2 above.

4. Unless otherwise noted, the information contained in this affidavit is based upon my personal knowledge and investigation of the above described offenses, the review of evidence obtained during the course of this investigation that includes information disclosed to me by other agents, investigators, chemists, and auditors, and my experience and background as a special agent for the FDA/OCI. As will be shown in this affidavit, I have probable cause to believe that the owner and employees of I FORCE have violated the Federal Food, Drug, and Cosmetic Act and the Controlled Substances Act in the commission of the following crimes:

a. The introduction or delivery for introduction into interstate commerce of an unapproved new drug in violation of 21 U.S.C. § 331(d);

b. The introduction or causing the introduction of misbranded drugs in interstate commerce in violation of 21 U.S.C. § 331(a);

c. The receipt in interstate commerce of a drug that is misbranded, and the delivery or proffered delivery thereof for pay or otherwise in violation of 21 U.S.C. § 331(c);

d. The doing of any act to a drug, while such a drug is held for sale after shipment in interstate commerce, which results in the drug being misbranded in violation of and 21 U.S.C. § 331 (k);

e. The failure to register as a drug manufacturer or list the drugs produced with the FDA in violation of 21 U.S.C. § 331(p);

f. The unlawful manufacture, distribution, or dispensing of, or possession with intent to manufacture, distribute, or dispense, a controlled substance in violation of 21 U.S.C. § 841(a)(1).

//

//

II. APPLICABLE PROVISIONS OF LAW

5. The FDA is the agency of the United States responsible for enforcing the provisions of the Federal Food, Drug, and Cosmetic Act ("FD&C Act"), 21 U.S.C. § 301 et seq. Among the purposes of the FD&C Act is to ensure that drugs sold for administration to humans, or for other use by or on humans, provide reasonable assurances of safety and effectiveness, and bear labeling containing only true and accurate information.

6. This investigation involves the manufacture and distribution of specially designed synthetic anabolic steroids, specifically Madrol, Superdrol, and androstenedione. Madrol is also known as "desoxymethyltestosterone" or "DMT" and has the chemical names 17a-methyl-5a-androst-2-en-17b-ol and 17-a-methyl-etioallocholan-2-ene-17b-ol, among others. Superdrol is also known as "Methasteron", "Methyldrostanolone", or "17a-Methyldrostanolone" and has the chemical names 2a,17a-dimethyl-5a-androstane-3-one-17b-ol, 2a, and 17a-dimethyl-etiocholan-3-one-17b-ol. Madrol and Superdrol are specially designed synthetic steroids and are derived from a simple chemical modification of another known steroid. The FDA's Center for Food Safety and Applied Nutrition has determined, through the analysis of other commercially available products containing Madol and Superdrol, that these two chemical substances are drugs, and not dietary supplements. Androstenedione, the third substance involved in this investigation, is a Schedule III Controlled Substance androstenedione.

7. Under the FD&C Act, a "drug" includes articles (other than food) which (1) are intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease in man, and (2) are intended to affect the structure or function of the body of man. Title 21, United States Code, Section 321(g)(1)(B)-(C).

8. A "new drug" is any drug which is not generally recognized, among experts qualified by scientific training and experience to evaluate the safety and effectiveness of drugs, as safe and effective for use under the conditions prescribed, recommended, or suggested in the labeling thereof. 21 U.S.C.

//

//

§ 321(p)(1). In order to be lawfully marketed, sold, or dispensed in the U.S., a new drug had to be the subject of a New Drug Application ("NDA") which had been approved by the FDA. 21 U.S.C. § 355.

9. Under the FD&C Act, certain drugs are defined as prescription drugs because (due to their toxicity and other potential harmful effects) they are not considered safe for use except under the supervision of a practitioner licensed by law to administer such drugs. 21 U.S.C. § 353(b)(l)(A)-(B). Because of their synthetic chemical structure and intended use, both Madrol and Superdrol qualify as "drugs" as defined at 21 U.S.C. § 321(g), and as "prescription drugs" as defined at 21 U.S. C. § 353(b)(1). Dispensing of a prescription drug without a valid prescription is an act which results in the drug being misbranded while held for sale. 21 U.S.C. § 353(b). Anabolic steroids are Schedule III Controlled Substances (21 U.S.C. § 812(b), Schedule III (e); 21 C.F.R. § 1308.13(f)). Anabolic steroids are also prescription drugs pursuant to 21 U.S.C. § 353(b)(1)(A).

10. Under the FD&C Act, a drug is deemed to be misbranded, under the following circumstances:

a. its labeling is false or misleading in any particular in violation of 21 U.S.C. §352(a);

b. its labeling lacks adequate directions and/or warnings for use in violation of 21 U.S.C. §352(f)(1) and (2);

c. the drug is dangerous to health when used in the dosage and manner and with the frequency and duration prescribed, recommended, and suggested on the labeling in violation of 21 U.S.C. § 352(j); or

d. the drug is manufactured, prepared, propagated, compounded, or processed in a facility that is not properly registered with FDA, or the drug is not included on the FDA's list of drugs manufactured in a properly registered facility in violation of 21 U.S.C. § 352(o).

11. Under the FDCA, every person engaging in the manufacture, preparation, compounding, or processing of drugs is required to immediately register with the FDA. 21 U.S.C. § 360(c). The terms "manufacture, preparation, propagation, compounding, or processing" include repackaging or otherwise changing the container, wrapper, or labeling of any drug in furtherance of the distribution of the drug from the original place of manufacture to the person who makes the final sale to the ultimate consumer or user. 21 U.S.C. § 360(a)(l).

//

12. Under the FD&C Act, the term "dietary supplement" is defined as a product intended to supplement the diet that bears or contains one or more of the following dietary ingredients: (a) a vitamin; (b) a mineral; (c) an herb or other botanical; (d) an amino acid; (e) a dietary substance for use by man to supplement the diet by increasing the total dietary intake; or (f) a concentrate, metabolite, constituent, extract, or combination of any ingredient described in clause (a), (b), (c), (d) or (e). 21 U.S.C. § 321(ff)(1). Any product containing either Madrol or Superdrol and labeled as a "dietary supplement" is fraudulently labeled. Madrol and Superdrol are synthetic compounds, not found in nature and do not meet the definition of a dietary supplement found at 21 U.S.C. § 321(ff).

13. Like Madrol and Superdrol, androstenedione is not a dietary supplement. Since January 20, 2005, it has been classified as a Schedule III Controlled Substance. The Steroid Control Act of 2004 amended the definition of a "anabolic steroid" found in the Controlled Substance Act, 21 U.S.C. § 802(41)(A) to mean any drug or hormonal substance, chemically and pharmacologically related to testosterone (other than estrogens, progestins, corticosteroids, and dehydroepiandrosterone), and specifically included androstenedione, defined as 1-androstenedione ([5"]-androst-1-en-3,17-dione; 4-androstenedione (androst-4-en-3,17-dione); 5-androstenedione (androst-5-en-3,17-dione); and "any salt, ester, or ether of a drug or substance described in this paragraph."

III. UNDERCOVER PURCHASES

14. In October of 2007, FDA/OCI Special Agent Robert Blenkinsop initiated an investigation into WWW.BODYBUILDING.COM, based on allegations that the website was involved with the unlawful distribution of unapproved new drugs, to include specially designed synthetic anabolic steroids. Subsequent to initiation of this investigation, your affiant was assigned as a co-case agent responsible for the I FORCE portion of this investigation.

15. On February 19, 2008, Agent Blenkinsop purchased I FORCE "Dymethazine" from WWW.BODYBUILDING.COM. He paid with a credit card, and used a California shipping address. The I FORCE "Dymethazine" was shipped from the WWW.BODYBUILDING.COM warehouse located in Boise, ID on February 9, 2009 to an address in California.

//

//

16. On February 19, 2008, Agent Blenkinsop reviewed the WWW.BODYBUILDING.COM website marketing page for the product "Dymethazine." This web page identified the ingredient in "Dymethazine" as 15mg of "Dymethazine™ "and included a list of the active ingredients, directions, warnings, and other marketing language which indicated that the product's intended use was to affect the structure or function of the body. This web page stated:

> With Dymethazine, you can expect gains in both size and strength, that will continue on for the duration of your cycle. This comes from the pro-hypertrophic effects of androgen receptor activation, nitrogen retention, and glycogen supercompensation. The combination of these powerful anabolic processes creates an environment for gains in muscle size and strength that are unlike anything you have ever experienced.

The following directions for use were included: "Cycle this product for 4-6 weeks; do not exceed 6 weeks continuous consumption."

17. Agent Blenkinsop subsequently examined the label on the I FORCE Dymethazine purchased from WWW.BODYBUILDING.COM. The label stated, "Mfg. For Dist. By: Tribravus Enterprises, LLC Escondido, CA 92029." The label also stated, "We are proud to announce the next generation of Designer Anabolics. Designer Anabolics are unique compounds that greatly increase the body's ability to induce myotropic (muscle building) effects." The label also warns, "[p]ossible side effects include acne, hair loss, growth on the face (in women), aggressiveness, irritability, and increased levels of estrogen."

18. Agent Blenkinsop submitted the I FORCE Dymethazine to the FDA's Forensic Chemistry Center for analysis, which included using a gas chromatography-mass spectrometry (GC-MS) screening. On March 24, 2009, the lab completed its analysis and determined that I FORCE Dymethazine contained Superdrol.

19. On April 10, 2009, Agent Blenkinsop accessed WWW.BODYBUILDING.COM and purchased I FORCE 1,4 AD Bold 200. He paid using a credit card and a shipping address in California. Agent Blenkinsop received the I FORCE 1,4 AD Bold 200 on April 13, 2009. The box was shipped by U.S.P.S. Priority Mail and had the return address "WWW.BODYBUILDING.COM, 5957 Vandal Way, Boise, ID, 83709."

20. On April 10, 2009, Agent Blenkinsop reviewed the WWW.BODYBUILDING.COM website marketing pages corresponding to I FORCE 1,4 AD Bold 200. These materials included a list

of the active ingredients, directions, warnings, and other marketing language which demonstrated that the intended use of the products was to affect the structure and/or function of the body. According to the website,

> This naturally occurring compound is a direct precursor to Boldenone, a derivative of testosterone. 1,4AD BOLD is an extremely effective aid for increasing receptor activation and initiating the muscle tissue rebuilding process that yields solid gains in lean muscle mass.

The directions stated, "[a]s a dietary supplement cycle as follows: Take 1 capsule twice daily. 1 capsules [sic] 30 minutes prior to training. Cycle for 6-8 weeks, then take 6-8 weeks off." The website warns that, "[p]ossible side effects include acne, hair loss, growth on the face (in women), aggressiveness, irritability, and increased levels of estrogen."

21. Agent Blenkinsop examined the label for the I FORCE 1,4 AD Bold 200 which included, "I FORCE Nutrition Mfg. For Dist. By Tribravus Enterprises, LLC Escondido, CA 92029." The list of ingredients, directions, and warnings included on this label appeared to be the same as those found on the WWW.BODYBUILDING.COM website at the time the product was purchased.

22. Agent Blenkinsop submitted the I FORCE 1,4 AD Bold 200 to the FDA's Forensic Chemistry Center for analysis. On June 5; 2009, the lab completed its analysis and determined that 1,4 AD Bold 200 contained Androstenedione, a Schedule III Controlled Substance.

23. On August 6, 2009, Agent Blenkinsop purchased I FORCE Products 1,4 AD Bold 200, 17a PheraFLEX, Dymethazine, and Methadrol from WWW.BODYBUILDING.COM. Agent Blenkinsop used a credit card and a California shipping address. He received the I FORCE products on August 8, 2009. The box was shipped via U.S.P.S. Priority Mail and had the return address "WWW.BODYBUILDING.COM, 5957 Vandal Rd., Boise, ID, 83709."

24. On August 6, 2009, Agent Blenkinsop reviewed the WWW.BODYBUILDING.COM website marketing pages corresponding to Dymethazine and 1,4 AD Bold 200. They contained the same misrepresentations that he found when he reviewed the website on February 9, 2009, and April 10, 2009.

25. On August 6, 2009, Agent Blenkinsop also reviewed the marketing pages corresponding to 17a PheraFLEX and Methadrol. According to the website, 17a PheraFLEX "[p]romotes Lean Muscle Gains!" The active ingredient listed on the website is 15mg of 17a-Methyl-Etioallocholan-

2-Ene-17b-Ol. The directions include, "[d]o not use for more than 3 weeks at a time." Warnings on the website identify possible side effects as, "acne, hair loss, growth on the face (in women), aggressiveness, irritability, and increased levels of estrogen." The Methadrol marketing on the website included the statement "[e]ffective Ingredient . . . An Extremely Active Designer Supplement!!" The active ingredient is listed as 10 mg of 2a, 17a DI Methyl Etiocholan 3-One, 17b-Ol. The directions and warning sections for Methadrol are the same as those listed for 17a PheraFLEX.

26. Agent Blenkinsop submitted the I FORCE 1,4 AD Bold 200, 17a PheraFLEX, Dymethazine, and Methadrol to the FDA's Forensic Chemistry Center for analysis. On September 1, 2009 the lab completed its analysis and determined that I FORCE 1,4 AD Bold 200 contained androsteneione; I FORCE 17a PheraFLEX contained Madol; and I FORCE Dymethazine and Methadrol both contained Superdrol.

27. Below is a chart summarizing the FDA purchases and lab analysis of I FORCE products:

PRODUCT	PURCHASE DATE	LAB ANALYSIS
Dymethazine	2/19/09	Superdrol
1,4 AD Bold 200	4/10/09	Androstenedione
Dymethazine	8/6/09	Superdrol
1,4 AD Bold 200	8/6/09	Androstenedione (Sched. III
17a PheraFLEX	8/6/09	Madol
Methadrol	8/6/09	Superdrol

28. On September 21, 2009, Agent Blenkinsop reviewed the FDA Electronic Orange Book, and determined that none of these products have been approved by the FDA. As "new drugs," these I FORCE products must be approved by FDA before they can be lawfully marketed pursuant to 21 U.S.C.§ 355. All approved drug products are listed in the FDA Orange Book of Approved Drug Products.

IV. I FORCE IN VISTA, CA

29. All food facilities, including firms manufacturing dietary supplements, are required to register their place of business with the FDA, and to notify the FDA of any changes of address. 21 U.S.C. § 350d. Agent Blenkinsop conducted a search of these food registration records for a registration by I FORCE. These records indicate I FORCE is registered as a food establishment, and its address, as

reported to the FDA, is 101 State Place, Suite A, in Escondido, CA. TRIBRAVUS ENTERPRISES is also registered with the FDA at the same address.

30. I have reviewed FDA import records, current as of March 26, 2009, which indicate that I FORCE and TRIBRAVUS ENTERPRISES have imported six shipments from China, the beginning on July 5, 2008, and continuing until February 20, 2009. These six shipments totaled 132.30 kilograms of what appear to be powders used as raw materials. I know from training and experience that many manufacturers of drugs and dietary supplements source raw materials from China for use in their manufacturing.

31. In November of 2006, the DEA investigated I FORCE and its owner, DAVID NELSON, for the unlawful importation of 3 ½ kilograms of the compound 1,4 androstadienedione. This investigation determined that I FORCE's business address was 101 State Place, Suite A, Escondido, CA, and NELSON's home address was 538 Chesterfield Circle, San Marcos, CA. This investigation determined that NELSON sent wire transfers to China for the purchase of raw materials, using a TRIBRAVUS ENTERPRISES bank account.

32. On August 6, 2009, I conducted surveillance at the State Place address. I noted that the parking space in front of the unit was marked "Tribravus," and I observed a U.P.S. attempted delivery notice and a peach-colored U.S. Postal Service Notice of Delivery form (PS 3849) for a parcel bearing tracking number EE132597741CN affixed to the door marked Suite A at 101 State Place, Escondido, CA. The name plate had been removed from the door and I determined the unit was vacant by looking through the front window.

33. The U.S. Postal Service Tracking and Confirmation Internet site confirmed that the parcel bearing Tracking Number EE132597741CN was delivered on August 7, 2009. The item was signed for by "A. Wisc." According to the Internet site the parcel had originated in Shanghai China and entered the U.S. at the San Francisco Airmail Facility.

34. On the morning of August 10, 2009, FDA/OCI Agents conducted surveillance of DAVID NELSON, and followed him from his residence located at 538 Chesterfield Circle in San Marcos, CA, to 1305 Hot Spring Way in Vista, CA, a commercial office complex. NELSON was observed entering

Suite 103. There were no markings on the building or suite entrance denoting I FORCE. A roll up garage door was observed on the west side of the unit.

35. Later on August 10, 2009, FDA/OCI Agents followed NELSON to a local restaurant, where NELSON was joined by six other males. Two of these males were wearing t-shirts emblazoned with "I FORCE." These seven individuals were overheard discussing product formulations, ingredients, etc.

36. At approximately 1:10 p.m., FDA/OCI Special Agent Liam Gimon, acting in an undercover capacity, entered the business located at 1305 Hot Spring Way, Suite #103, Vista, CA. When Agent Gimon first entered the business, he observed a computer located in the reception area. Inside the business, Agent Limon encountered DAIVA GEDGAUDAS and spoke with her about I FORCE's business. The information set forth in paragraphs 37 and 38 was provided voluntarily by GEDGAUDAS.

37. GEDGAUDAS identified herself as the wife of the owner, "Dave." GEDGAUDAS said she was employed by her husband, in his sports supplement company, located in the suite. GEDGAUDAS stated that her husband's sport supplement company had just moved into the suite last week, and that they had just gotten the phone system up and running the night before. GEDGAUDAS provided Agent Gimon with a business card for Alec Wisecup. GEDGAUDAS identified Wisecup as in charge of the office and said he would be able to answer any questions about the office or the business. The business card identified the company as "I FORCE NUTRITION, TRIBRAVUS ENTERPRISES, LLC, 101 State Place, Suite A, Escondido, CA 92029, www.IFORCEnutrition.com, alec@IFORCEnutrition.com. GEDGAUDAS handwrote "WWW.BODYBUILDING.COM" on the reverse of the card.

38. GEDGAUDAS informed Agent Gimon that her husband's company sells sports supplements to wholesalers, not to individuals or end users. According to GEDGAUDAS, their largest buyer is WWW.BODYBUILDING.COM, and the site offers the best prices for their products. They sell some of their products to local stores, but GEDGAUDAS was unsure as to which local stores carried their products. According to GEDGAUDAS, her husband has been in the sports supplement business for years, originally as a distributor. GEDGAUDAS stated that he now sold only to wholesalers.

GEDGAUDAS also stated that IFORCE obtains its ingredients from China. GEDGAUDAS provided that they have had issues with the quality of their ingredients in the past and now sometimes submit them to a laboratory for analysis. IFORCE sends the ingredients to an encapsulator, who puts the powder ingredients into capsule form. The encapsulator is located in the building next door to the office. GEDGAUDAS noted that was very convenient having them there. The encapsulator mails the products directly from their factory to customers.

V. DOCUMENTARY AND DIGITAL EVIDENCE

39. Having conducted numerous search warrants of businesses, I know that it is routine for businesses to keep records, including sales records, contracts, invoices, financial records, shipping records, phone records, at their residence and place of business, often for long periods of time. These records typically include bank statements, check books, debit cards, credit cards and other bank records, all of which can be of assistance in identifying financial transactions involving illicit revenue. It is also routine for individuals and businesses to retain cell phones, phone books, rolodexes, notes, phone numbers and addresses, phone bills and other phone-related material, which can further help to identify illegal distributions of controlled substances and misbranding violations of the FDCA. I am also aware that under several sections of the FDCA, firms regulated by the FDA are required to retain documents related to the products they manufacturer and/or distribute. I also know that companies in this business, like most other companies, routinely maintain the above described records electronically. Furthermore, most companies in this business have computerized operations with automated billing, shipping, and receiving processes.

VI. PROCEDURES FOR ELECTRONICALLY STORED INFORMATION

40. With the approval of the Court in signing this warrant, agents executing this search warrant will employ the following procedures regarding computers and other electronic storage devices, including electronic storage media, that may contain data subject to seizure pursuant to this warrant:

Incremental Search

a. IFORCE is a functioning company with numerous employees. A seizure of the company's computer network may have the unintended and undesired effect of limiting the company's ability to provide lawful services to its legitimate customers. Consequently, the agents who execute the

search will take an incremental approach to minimize the inconvenience to the company's customers and to minimize the need to seize equipment and data. This incremental approach, which will be explained to all of the agents on the search team before the search is executed, will proceed as follows:

i. Upon arriving at the business to execute the search, the agents will attempt to identify a system administrator of the network (or other knowledgeable employee) willing to assist law enforcement with the identification of relevant systems and with the copying of computer files from network servers and other systems believed to contain information within the scope of the warrant. If the agents succeed at locating such an employee and are able to obtain copies of the relevant data in this fashion, the agents will not create a forensic image of the entire network. Imaging network servers is complex, time-consuming, usually interferes with legitimate business activities and legitimate access and can result in the acquisition of a veritable mountain of irrelevant data. Workstations and laptops believed to contain relevant data, however, may be imaged or taken for imaging offsite, as provided below.

ii. If the employees choose not to assist the agents, the search team will attempt to locate network servers and will attempt to identify relevant data stores including user directories, file shares, electronic mail accounts and logs and make electronic copies of the data stores reasonably believed to contain information subject to the warrant.

iii. If identifying and copying data stores onsite is technically or logistically not feasible, the entire server network may be imaged. As discussed below, whether the image is obtained onsite or offsite will be determined by technical issues, time-constraints and safety concerns. After the images are obtained, the data will be analyzed as provided below.

iv. To the extent that information within the scope of this warrant may be found not only on servers but also on personal computers, workstations, laptops and other electronic storage devices which may be located at the business, such computers devices will be forensically imaged onsite or offsite as provided below.

//

//

//

Forensic Imaging

b. After securing the premises, or if sufficient information is available pre-search to make the decision, the executing agents will determine the feasibility of obtaining forensic images of electronic storage devices while onsite. In making this determination, the executing agent will not access any data stored on the device(s). A forensic image is an exact physical copy of the hard drive or other media. A forensic image captures all of the data on the hard drive or other media without the data being viewed and without changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of the data for information subject to seizure pursuant to this warrant. The feasibility decision will be based upon the number of devices, the nature of the devices, the volume of data to be imaged, the need for and availability of computer forensics specialists, the availability of the imaging tools required to suit the number and nature of devices found and the security of the search team. The preference is to image onsite if it can be done in a reasonable amount of time and without jeopardizing the integrity of the data and the safety of the agents. The number and type of computers and other devices and the number, type and size of hard drives are of critical importance. It can take several hours to image a single hard drive - the bigger the drive, the longer it takes. As additional devices and hard drives are added, the length of time that the agents must remain onsite can become dangerous and impractical.

c. If it is not feasible to image the data on-site, computers and other electronic storage devices, including any necessary peripheral devices, will be transported offsite for imaging. After verified images have been obtained, the owner of the devices will be notified and the original devices returned within forty-five (45) days of seizure absent further application to this court.

Segregation and Extraction of Data

d. After obtaining a forensic image, the data will be analyzed to locate, segregate and extract data subject to seizure pursuant to this warrant. Analysis of the data following the creation of the forensic image can be a highly technical process requiring specific expertise, equipment and software. There are literally thousands of different hardware items and software programs, and different versions of the same program, that can be commercially purchased, installed and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical

computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

e. Analyzing the contents of a computer or other electronic storage device, even without significant technical challenges, can be very challenging. Searching by keywords, for example, often yields many thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue: who created it, when and how it was created or downloaded or copied, when was it last accessed, when was it last modified, when was it last printed and when it was deleted. Sometimes it is possible to recover an entire document that never was saved to the hard drive if the document was printed. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search text. Many common electronic mail, database and spreadsheet applications do not store data as searchable text. The data is saved in a proprietary non-text format. Documents printed by the computer, even if the document never was saved to the hard drive, are recoverable by forensic programs but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. Similarly, faxes sent to the computer are stored as graphic images and not as text. In addition, a particular relevant piece of data does not exist in a vacuum. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted or printed the data requires a search of other events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which user had logged in, whether users share passwords, whether the computer was connected to other computers or networks, and whether the user accessed or used other programs or services in the time period surrounding events with the relevant data can help determine who was sitting at the keyboard.

f. Analyzing data has become increasingly time-consuming as the volume of data stored on a typical computer system and available storage devices has become mind-boggling. For example, a single megabyte of storage space is roughly equivalent of 500 double-spaced pages of text.

A single gigabyte of storage space, or 1,000 megabytes, is roughly equivalent of 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal computers capable of storing up to 2 terabytes (2,000 gigabytes) of data. And, this data may be stored in a variety of formats or encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer). The sheer volume of data also has extended the time that it takes to analyze data. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. And, once reviewed, relevant data leads to new keywords and new avenues for identifying data subject to seizure pursuant to the warrant.

g. Based on the foregoing, segregating and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including hashing tools specific to identifying data subject to seizure pursuant to this warrant, and may take weeks or months. The personnel conducting the segregation and extraction of data will complete the analysis and provide the data authorized by this warrant to the investigating team within ninety (90) days of imaging, absent further application to this court.

h. All forensic analysis of the imaged data will employ search protocols directed exclusively to the identification, segregation and extraction of data within the scope of this warrant. The personnel conducting the segregation and extraction will not communicate to the investigating team any information learned during the analysis that is outside the scope of the warrant. In the event that the personnel lawfully conducting the analysis identify information pertaining to crimes outside the scope of the warrant, such information will not be disclosed to the investigating team or used in any way unless a new warrant is obtained to search for such information. The new warrant may be sought by the analyst, if he or she is a sworn federal agent, or by an agent not part of the original investigating team. A federal prosecutor apart from the original investigating team will be assigned to assist in determining whether to apply for a new warrant and in obtaining such a warrant. Absent a new warrant, the segregating personnel will only search for and seize data that they would be entitled to retain independent of the new information and the original investigating team will not use any data outside the scope of this warrant even if found in plain view.

//

Retention of an Image

i. As mentioned above, a forensic image of a hard drive or other electronic storage device is an exact copy of the entire device. It is necessary to retain a forensic image of each electronic storage device that was subjected to analysis for a number of reasons including, but not limited to, proving authenticity of evidence to be used at trial, responding to questions regarding corruption of data, establishing chain of custody of data, refuting claims of fabricating, tampering or destroying data, and, addressing potential Brady claims where, for example, a defendant may claim that the government avoided its obligations by destroying data or returning it to a third party. The retained image or images will be sealed and only accessed upon further order of a court of competent jurisdiction.

Return of Search Warrant

j. Following the execution of this warrant a return will be submitted to the court reflecting the physical inventory as provided at Rule 41. Within fourteen (14) days of data being provided to the investigating team from the segregation and extraction team, the government will submit a certification to the court: (1) identifying the data provided to the investigating team and the date that it was provided; (2) certifying that only a single forensic image of each device was retained as authorized at subparagraph (h) above; (3) certifying that only data believed subject to seizure pursuant to this warrant was provided to the investigating team; and, (4) certifying that the original devices and any copies made by the government have either been destroyed or returned to the owner. If the data provided to the investigating team was provided in electronic form, it will be sufficient identification of that data for the government to provide a true copy of the electronic storage media containing the data to the court sealed in a manner to protect its integrity and appropriate for filing.

Genuine Risks of Destruction

k. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, electronically stored data can be permanently deleted or modified by users possessing basic computer skills. In this case, only if the subject receives advance warning of the execution of this warrant, will there be a genuine risk of destruction of evidence. In this case, search warrants were executed on September 24, 2009 at 10:00 a.m. in other associated business locations outside the Southern District of California. Based on my training and experience, I believe it

is likely that I FORCE has been notified of the execution of these search warrants. This fact increases the risk of destruction of evidence.

Prior Attempts to Obtain Data

l. The United States has not attempted to obtain this data by other means.

User-Attribution

m. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, it is often difficult or impossible to determine the identity of the person using the computer when incriminating data has been created, modified, accessed, deleted, printed, copied, uploaded or downloaded solely by reviewing the incriminating data. Computers generate substantial information about data and about users which generally is not visible to users. Computer-generated data, including registry information, computer logs, user profiles and passwords, web-browsing history, cookies and application and operating system metadata, often provides evidence of who was using the computer at a relevant time. In addition, evidence such as electronic mail, chat sessions, photographs and videos, calendars and address books stored on the computer may identify the user at a particular, relevant time. The manner in which the user has structured and named files, run or accessed particular applications, and created or accessed other, non-incriminating files or documents, may serve to identify a particular user. For example, if an incriminating document is found on the computer but attribution is an issue, other documents or files created around that same time may provide circumstantial evidence of the identity of the user that created the incriminating document.

n. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, electronically stored data can be permanently deleted or modified by users possessing basic computer skills. In this case, only if the subject receives advance warning of the execution of this warrant, will there be a genuine risk of destruction of evidence.

VII. CONCLUSION

41. Based on the information provided in this affidavit, I FORCE is involved in the illegal manufacture and distribution of unapproved new drugs, misbranded drugs, and controlled substances namely, Dymethazine, 1,4 AD Bold 200, 17a PheraFLEX, and Methadrol, in violation of 21 U.S.C. § 331 (a), (c), (d), (k), and (p) and 21 U.S.C. § 841(a)(1). I have probable cause to believe that evidence

of these violations, as described in more detail at Attachment B to this affidavit, exists at I FORCE's business location at 1305 Hot Spring Way, Suite #103, Vista, CA, which is more particularly described in Attachment A to this affidavit.

I declare under penalty of perjury that the foregoing is true and correct.

Lisa Hartsell, Special Agent
FDA-Office of Criminal Investigations

Sworn to and subscribed before me
this 24 th day of September, 2009.

HONORABLE LOUISA S. PORTER
United States Magistrate Judge

EXHIBIT G

Food and Drug Administration
OFFICE OF CRIMINAL INVESTIGATIONS
REPORT OF INVESTIGATION

REPORTING OFFICE:	Seattle Domicile Office
DOCUMENT NUMBER:	181135
CASE NUMBER:	2011-SEW-715-0059
RELATED CASE NUMBER:	
TYPE OF CASE:	715.100, MISBRANDED PRODUCTS - CDER
CASE TITLE:	PROJECT GREEN LIFE
CASE AGENT:	DALI BORDEN
INVESTIGATION MADE AT:	Kirkland, WA
INVESTIGATION MADE BY:	SA DaLi Borden
REPORTING PERIOD:	**FROM:** 10/28/2010 **TO:** 11/29/2010
STATUS OF CASE:	Continued
SYNOPSIS:	Opening report. Several undercover sales were initiated and received. Agents located the Post Office used by subjects. Agent met with AUSA.

RESTRICTED INFORMATION

This report is furnished on an official need-to-know basis and must be protected from dissemination which might compromise the best interests of the Food and Drug Administration, Office of Criminal Investigations. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the FDA Office of Criminal Investigations.

UNAUTHORIZED RELEASE MAY RESULT IN CRIMINAL PROSECUTION

REPORT SUBMITTED BY: _____ DATE: 11/29/2010
DaLi Borden, Special Agent

REPORT APPROVED BY: _____ DATE: 12-6-10
Thomas W. Emerick, Special Agent in Charge

DISTRIBUTION:
ORIG: SFC
CC: LAC
CC: AD-IOD
CC: SEW

[redacted]

[redacted]

On 11/18/10, SA Borden received a copy of PGL's "Membership Contract" provided to SA Hartsell when she joined the PGL ".. Private Healthcare Membership Association." See Attachment 3. The document lists as the Association's first objective to "....protect our rights to freedom of choice regarding our health information and care, through maintaining our Constitutional rights."

[redacted]

EXHIBIT H

4

Food and Drug Administration
OFFICE OF CRIMINAL INVESTIGATIONS
REPORT OF INVESTIGATION

REPORTING OFFICE:	Seattle Domicile Office
DOCUMENT NUMBER:	188752
CASE NUMBER:	2011-SEW-715-0059
RELATED CASE NUMBER:	
TYPE OF CASE:	715.100, MISBRANDED PRODUCTS - CDER
CASE TITLE:	PROJECT GREEN LIFE
CASE AGENT:	DALI BORDEN
INVESTIGATION MADE AT:	Kirkland, WA
INVESTIGATION MADE BY:	SA DaLI Borden
REPORTING PERIOD:	**FROM:** 11/30/2010 **TO:** 02/25/2011
STATUS OF CASE:	Continued
SYNOPSIS:	Information received from Stamps.Com, and bank account information identified. OCL will be lead on the case in Eastern District of Washington. Packaging location identified.

RESTRICTED INFORMATION

This report is furnished on an official need-to-know basis and must be protected from dissemination which might compromise the best interests of the Food and Drug Administration, Office of Criminal Investigations. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the FDA Office of Criminal Investigations.

UNAUTHORIZED RELEASE MAY RESULT IN CRIMINAL PROSECUTION

REPORT SUBMITTED BY: _____ DATE: 02/25/2011
DaLi Borden, Special Agent

REPORT APPROVED BY: _____ DATE: 3/2/11
Thomas W. Emerick, Special Agent In Charge

DISTRIBUTION:
ORIG: SFC
CC: LAC
CC: AD-IOD
CC: SEW

AGENT COPY

On 01/21/11, SA Borden was contacted by OCL Attorney Jeff Steger inquiring about the investigation. Steger indicated he would consult with his supervisor and likely contact AUSA Harrington, EDWA, to see if Steger could be of assistance.

On 02/01/11, Jeff Steger, OCL, contacted the SA Borden after he consulted with AUSA Harrington, EDWA. Steger had contacted the AUSA to offer assistance in the EDWA investigation if Harrington was ready to pursue the case or to advise Harrington of OCL's interest in the investigation. Steger advised SA Borden that AUSA Harrington wanted to have a conference call to review the status of the investigation on 02/08/11.

From 02/02 to 02/04/11, SA Borden assembled a briefing document regarding the investigation to date, for the conference call.

On 02/08/11, SA Borden organized a conference call with the AUSA from EDWA, Trial Attorney Steger, OCL, Jim Smith, OCC, and Investigator Bega, USPIS. The attorneys and investigators discussed the investigation to date and the attorneys asked questions related the violations of the FDCA.

02/15/11, Trial Attorney Steger, OCL, advised SA Borden that OCL would take the lead on this investigation. Trial Attorney Chris Parisi had been assigned the case will be working on the matter. EDWA has offered administrative support and help with Grand Jury, subpoenas, and anything else that comes up.